Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

"THE PRESENT CYBER INFRASTRUCTURE AND GROWING DEPENDENCE ON CYBER TECHNOLOGY DEMANDS CYBERSECURITY TO BE A NATIONAL AND ECONOMIC SECURITY PRIORITY"

Nityash Solanki
Ph.D. Scholar & Founder of "ONSHI"
Department of Law, Jagannath University, Jagannath University
Email ID: nityashsolanki@gmail.com

ABSTRACT

The ever-expanding and increasing number of illegal and unacceptable cyber intrusions and instances are continuously posing a major threat to the present cybersecurity systems used by federal authorities and private sectors. As a result, Americas cyber space is constantly under attack. Efforts by The Department of Homeland Security that was created to maintain and resolve cyber irregularities while protecting networks and cyberdata has shown some failure to devise effective regulations to safeguard the cyber space. The increasing number of successful efforts by hackers, group of hackers, business competetors, organized crime groups, terrorirsts all around the world have infected and disabled computers to steal sensetive data followed by improper disclosures, privacy breaches, identity thefts and financial thefts. The United States Congress is now burdened with the task and responsibility to legislate cybersecurity measures designed to prevent the undesirable cyber attacks on the private as well as government sectors. Moreover, the fact that the recent attempts to determine the working of cybersecurity regulation i.e. The Cybersecurity Act of 2012, which is going through lot of debates and analysis to baseline security standards to address various cyber related issues has shown some seriousness on the government's part to fame a completely satisfactory Cybersecurity Act to prevent damages to country's assets and losing sensitive information.

Keywords: *Cybersecurity, Department of Homeland Security, Hackers, Digital Communication, Internet, Awareness Campaign*

INTRODUCTION

Since the world has moved into the new century, we have seen an exponential growth in cyber technologies. Our increasing reliance and dependence on the Internet technology in our day-to-day affairs[1] has resulted is frequent usage when it comes to working professionally.[2] Before anyone could realize, the widespread use and dependence on the Internet technology turned it into an essential and integral part of global, national, and local economy.[3] In any event, this increasing dependence on technology has enabled our enemies in cyberspace (i.e. individual or group of

[1] Yee Fen Lim, *"Cyberspace law Commentaries and Material,"* Oxford University Press, 1-5 (2d ed. 2007).
[2] Jonathan Clough, *"Principles of Cybercrime,"* Cambridge University Press, 3-4 (2011).
[3] Tara O'Toole, *"Ensuring a Safe Cyberspace Through Research and Development,"* The Department of Homeland Security, (Oct. 21, 2012), http://www.dhs.gov/blog/2012/10/26/ensuring-safe-cyberspace-through-research-and-development (last visited Nov. 29, 2012).

hackers or business competitors or organized crime groups or terrorists) to infect and disable computers putting sensational data to risk of loss by improperly disclosing it through privacy breach or identity theft in cyberspace.[4]

Adoption of the new and innovative interconnected network regime or system at home or at work illustrates our increasing dependence on technology. Our thirst for growth and development led the malevolent hackers and cyber security risks and threats to enter our systems, at the same time, giving them multiple ways to gain access to information for financial or any other purposeful gains.[5] In 2009, President Obama issued Cyberspace Policy Review, which directed the Department of Homeland Securities (DHS) attention towards the need to create cybersecurity awareness campaign for illustrating to everyone the cybersecurity risks that await online.[6]

The types and frequency with which the cyber risks are floating in the present cyber world could be determined with the help of the following example: -

As part of the American's holiday season and Thanksgiving tradition the deals and bargains available on the 'online shopping day' of the year i.e. 'The Cyber Monday – the Monday after Thanksgiving' marks one of the biggest shopping days of the year.[7] Therefore, to prevent the cyber threats to privacy, the national public awareness campaign i.e. Stop. Think. Connect., intended for educating Americans of the safe Internet practicing habits, alluded to few safe online tips to avoid loss of personal information and transactions.[8]

Some of the safety tips to initiate public awareness included: - (1) Checking bank statements, (2) Using a credit card instead of a debit card, (3) Keeping computers up-to-date with new anti-virus and software, (4) Keeping a record of orders made online, (5) Buying from reputed sites and (6) Checking privacy policies online.[9]

In the present digital age, the risks, vulnerabilities and attacks that exist in the cyber world are not limited to any particular field. The ambit of the problem is reflected and seen affecting almost every government and private fields in the United States. According to the 2011 Internet usage census, U.S. secured the second position with the second highest number of Internet users in the world.[10] Consequently, the United States military authority has noticed 17-fold increase in

---

[4] U.S. Senate Committee, *"Senate Rejects Second Chance to Safeguard Most Critical Network, Homeland Security & Governmental Affairs,"* (Nov. 14, 2012), http://www.hsgac.senate.gov/media/majority-media/senate-rejects-second-chance-to-safeguard-most-critical-cyber-networks- (last visited Nov. 30, 2012).

[5] Stop.Think.Connect., The Department of Homeland Security, http://www.dhs.gov/stopthinkconnect (last visited Nov. 29, 2012).

[6] Id.

[7] *"Stop.Think.Connect.: Looking for Cyber Monday Scams,"* The Department Of Homeland Security, (Nov. 21, 2012), http://www.dhs.gov/blog/2012/11/21/stopthinkconnect-lookout-cyber-monday-scams (last visited Nov. 29, 2012).

[8] Id.

[9] *"Stop.Think.Connect.: Looking for Cyber Monday Scams,"* The Department Of Homeland Security, (Nov. 21, 2012), http://www.dhs.gov/blog/2012/11/21/stopthinkconnect-lookout-cyber-monday-scams (last visited Nov. 29, 2012). See also, Security Tip (ST07-001) *"Shopping Safely Online,"* United States Computer Emergency Readiness Team, (Dec. 6, 2010), http://www.us-cert.gov/cas/tips/ST07-001.html (last visited Nov. 29, 2012).

[10] *"Internet World States: Usage and Population Statistics,"* Internet World States, (June 30, 2012), http://www.internetworldstats.com/top20.htm (last visited Nov. 29, 2012).

cyber-attacks since 2009, either by hackers, criminal gangs or other nations.[11] General Keith B. Alexander's[12] evaluation reveals that increasing number of cyberattacks are aimed primarily on completely damaging "critical infrastructure" of the United State, as a result, America's (i) electricity grids, (ii) water supplies, (iii) computers and (iv) cell phone networks, are constantly under a threat of attack.[13] As a further matter, he shared the reality of the countrys state of readiness especially against such a large-scale cyberattack and although quite shocking, he placed the country's preparedness to be around 3, on a scale of 10.[14]

In spite of the fact that the situation demands responses, the Congress has no clear justification 'against' or 'in favor of' passing of Cybersecurity Act of 2012. In any event, the hackers are continuously trying to jump the technical barriers crossing and passing through all the lines that it is almost impossible for us to trace or track them down. The situation demands quick responses and to come up with new laws and policies relating to cybersecurity.

The brief on affairs extracted and discussed in this paper illustrate the difficulties faced, preventive measures adopted or suggested, and theoretical doctrines that should be adopted relating to cybersecurity to secure the country's present cyber space.

INTERNET, CYBERSPACE & THE WORLD WIDE WEB

Development and globalization strategies have been effectively carried out with the help of Internet and cyber technologies to stretch out to goals, which were a decade ago thought to be beyond country's reach or impossible to achieve. There is now on turning back from the present international communication system of a giant network that interconnects innumerable small groups of linked computer networks to access and exchange information, which was initially named ARPANET, and is now commonly known as the 'Internet'.[15] Internet technology first originated in 1969 as an experimental project of the Advanced Research Project Agency ('ARPA') that linked computer networks and computers owned by the defense contractors, military authorities and university laboratories to conduct defense-related research.[16] The global medium of communication that links computer and computer networks that are owned by government, public or private institutions, corporations, and non-profit organizations forms the 'cyberspace'.[17] The 'World Wide Web' technology allows access to series of documents and information, which is stored at different locations over the Internet involving numerous computers all around the world to come together and become part of a single body of knowledge. Access to the information stored as a single body of knowledge is made available through programs that 'browse' the Web and

[11] David E. Sanger, Eric Schmitt, *"Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure,"* N.Y. Times, July 27, 2012, at A8.
[12] Head of U.S. Cyber Command and National Security Agency.
[13] David E. Sanger, *supra* note 11.
[14] Id.
[15] *American Civil Liberties Union, et al v. Janet Reno, Attorney General of the United States,* 929 F. Supp 824, 831 (Dist. Ct. 1996).
[16] Id.
[17] Id.

display the hyperlinks attached to the formatting language called the hypertext markup language (HTML).[18]

HACKING COMPUTERS

The feeling of excitement attached to the growth and development of this technology clearly made everyone "as blind as a bat" leaving the country unprepared to the loopholes created by its growth. In the recent years, hackers committing cyber offenses have gained unauthorized access to computer systems causing damage and illegitimate interference and interception of data in order to impair or damage normal day-to-day operations of the computers and super computers used by an individual or government.[19] Gaining access to confidential data and information,[20] obtaining false identification documents[21] and creating false accounts[22] are some of the common frauds that are conducted by hackers using malicious software like viruses, worms, bots, spyware and Trojans.[23] In *United State v. Morris*, defendant was found guilty for inserting a worm designed to invade computers for which he had no authority or access. The defendant was convicted of violating The Computer Fraud and Abuse Act of 1986, because his act resulted in damaging computers in excess of $1,000.[24]

Some of the malicious software commonly used to infect computers includes virus, Trojan, worm, and bot. A virus is a program that infects computers by attaching itself to another program and once the virus is attached it runs with the so-called other program to perform the specific infecting functions on the computer.[25] A Trojan horse is a computer program that appears to be innocent at first but contains a hidden function of damaging or erasing hard disks that at the same time also allows hackers to perform system commands once the Trojan is installed on victim's computer.[26] A small piece of software that replicates itself using computer networks and security holes to scan the network of victim's computer is commonly known as a worm.[27] With the help of a computer program called 'bot', hackers can easily infect victim's computer and gain access to all the targeted computers remotely.[28]

For example, in *U.S. v. Clark,*[29] a 21-year-old defendant using a worm gathered more than 20,000 bots and directed them to connect to password-protected Internet relay chat (IRC) server

---

[18] Id.
[19] Jonathan Clough, *supra* note 2 at 27.
[20] *U.S. v. Kwak,* (D DC 2006), U.S. Department of Justice Press Release, (May 12, 2006), www.cybercrime.gov/kwakSent.htm. (last visited Nov. 20, 2012).
[21] *Hull v. WA,* [2005], WASCA 194.
[22] *U.S. v. An Unnamed Juvenile II* (D Mass 2005), U.S. Department of Justice, Press Release, (Sep. 8, 2005), www.cybercrime.gov/juvenileSentboston.htm. (last visited Nov. 20 2012).
[23] Jonathan Clough, *supra* note 2 at 32.
[24] 928 F.2d 504 (2nd Cir 1991).
[25] Marshall Brain and Wesley Fenlon, *"How Computer Viruses Work,"* How Stuff Works, http://computer.howstuffworks.com/virus.htm (last visited Nov. 30, 2012).
[26] Id.
[27] Id.
[28] Id.
[29] U.S. Department of Justice, Press Release (Dec. 28, 2005), http://www.justice.gov/criminal/cybercrime/cccases.html (last visited Nov. 26, 2012).

to launch DoS attack on computer networks connected to the Internet. Consequently, the defendant pleaded guilty of conducting the attack against the Internet auction site namely 'eBay'.[30]

CYBER INSTANCES

The hackers and malicious competitors are always a few steps ahead of us and all our efforts (i.e. through obsolete legislations and policies) to stop the attacks have unexpectedly resulted in failure to encounter the situation. The cyber instances and their impacts on different government authorities discussed in this section summarize how technology has facilitated individual or group of hackers around the world to hamper development, interfering in law enforcement, and other illegal activities including theft of sensitive or personal information.

Central Intelligence Agency (CIA)

In June 2011, a DDoS (Distributed Denial of Services) cyber-attack by LulzSec[31], an anonymous hacker group, managed to block access to the CIA (Central Intelligence Agency) website's homepage. Additionally, the hacker group also prevented access to FBI's phone network in Detroit alleging that the hacking act was done merely for fun.[32]

United States Congress

In June 2011, LulzSec broke into the Senate's website hacking public portions of the Senate's computer network. It was fortunate for the U.S. Senate that their website could not be brought to disrepute by the group.[33]

In March 2009, China-based hackers attacked Senator Nelson's personal office computer.[34]

In August 2006, China-based hackers successfully hacked four of the Wolf's personal office computers including computers of foreign policy staff and human rights staff, computers of his chief of staff, legislative director, and judiciary staff to gain access to information about human rights activities around the world.[35]

United States Department of Agriculture

In June 2006, the Department of Agriculture was hacked that allowed the hacker to access information of 26,000 Washington area employee's names, Social Security number with photos.[36]

United States Department of Commerce

---

[30] Id.

[31] Mostly targeting gaming sites.

[32] Marc Chacksfield, *"CIA Website and FBI Hacked by LulzSec,"* Techradar, (June 16, 2011), http://www.techradar.com/news/internet/cia-website-and-fbi-hackedby-lulzsec-966715 (last visited Nov. 16, 2012).

[33] Diane Bartz and Thomas Ferraro, *"Hackers Break into Senate Computers,"* Reuters, (June 13, 2011), http://www.reuters.com/article/2011/06/14/us-cybersecurity-usa-senate-idUSTRE75C5JI20110614 (last visited Nov. 16, 2012).

[34] Josh Rogin, *"Hackers Based in China Break into Florida Senator's Office Computers,"* Young Professionals in Foreign Policy, (March 24, 2012), https://ypfp.org/content/hackers-based-china-break-florida-senator's-office-computers (last visited Nov. 26, 2012).

[35] News release, *"Wolf Reveals House Computers Compromised by Outside Source,"* Frank Wolk, 10th District of Virginia, (June 11, 2008), http://wolf.house.gov/index.cfm?sectionid=34&parentid=6&sectiontree=6,34&itemid=1174 (last visited Nov. 26, 2012).

[36] "*Cyber Attacks Continue to Grow,"* MSNBC, (May 29, 2009), http://www.msnbc.msn.com/id/31000126/ns/technology_and_science-security/t/cyber-attacks-continue-grow/ (last visited Nov. 26, 2012).

In February 2012, the Department of Commerce was forced to disconnect the Internet from working because of a virus that was inserted into the Economic Development Administration's computer network.[37]

In December 2007, a spyware program was detected by computer-security expert on devices used by the Commerce Secretary Carlos Gutierrez that attempted to remove information and allowed communication channels through downloading contents from devices used by the Commerce Secretary, when he was in a meeting with the Joint Commission on Commerce and Trade in China to discuss matter such as intellectual property rights, market access and consumer product safety.[38]

In October 2006, computers used by the Bureau of Industry and Security (Department of Commerce) were hacked by unknown intruders using Chinese servers forcing the Department to lock down Internet access to their networks for several months compelling them to review U.S. export information and replacing hundreds of computers to thoroughly clean the devices from malicious codes.[39]

In February 2012, a spy group from China hacked conference calls with the intention to steal classified information on jet technologies. Consequently, the Commerce Department's Bureau of Industry and Security delayed and increased the F-35 Joint Strike Fighter's cost. The surprising part of this particular event was that the information system designed was without any protection against the cyber espionage making it an easy target.[40]

United States Department of Defense

In December 2011, RQ-170 stealth aircraft, a secret U.S. surveillance drone designed to infiltrate enemy's air defenses, was subjected to cyberattack and eventually crashed in Iran. RQ-170 played a vital role in the raid in which U.S. Navy SEALs killed Osama Bin Laden. Consequently, now the aircraft could be used by the Iranians to understand the stealth technology like how to design aircraft to trick radars or could also be used to better understand the vulnerabilities to U.S. stealth technology.[41]

In March 2011, a Defense Department contractor's computer was hacked and more than 24,000 files were stolen. Deputy Defense Secretary, William Lynn, while disclosing the Defense

---

[37] Lisa Rein, *"For Commerce Unit Hit by Computer Virus, Hardship of Being Unplugged Has Upside,"* The Washington Post, (April 9, 2012), http://www. washingtonpost.com/politics/for-agency-a-loss-of-technology-has-had-down--and-upsides/2012/04/08/gIQAvpAY5S_story.html (last visited Nov. 17, 2012).

[38] Shane Harris, *"China's Cyber-Militia,"* National Journal, (May 31, 2008), http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531 (last visited Nov. 24, 2012).

[39] Gregg Keizer, *"Chinese Hacker Hit Commerce Department,"* Information Week, (Oct. 6, 2006), http://www.informationweek.com/news/193105227 (last visited Nov. 18, 2012).

[40] *"Did Chinese Espionage Lead to F-35 Delays?"* Defense Tech, (Feb. 6, 2012), http://defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35- delays/ (last visited Nov. 29, 2012).

[41] Greg Jaffe and Thamos Erdbrink, *"Iran Says it Downed U.S. Stealth Drone; Pentagon Acknowledges Aircraft Downing,"* The Washington Post, (Dec. 4, 2011), http://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/ gIQAyxa8TO_story.html (last visited Nov. 26, 2012).

Department's cyberspace strategy mentioned that some of the stolen file included sensitive systems like aircraft avionics, surveillance technologies, satellite communication system, and network security protocols.[42]

In December 2010, an unknown hacker accessed personal information of 650 soldiers stored on a computer in Santa Fe, New Mexico.[43]

In April 2010, the Army lost personal data from a regional reserve command in Fort Totten. Hence, the Army warned 12,000 areas military and civilian personnel advising them to check credit bureau report and be aware about the likeliness of identity theft.[44]

In December 2009, militants in Iraq used $26 off-the-shelf, an inexpensive file-sharing computer program, to obstruct live video feeds of U.S. Predator Drones to successfully obtain access to the U.S. military operations by hacking information.[45]

In June 2007, some unknown hackers successfully compromised unclassified e-mail account of the Secretary of defense.[46]

In May 2007, intruders left spyware on The National Defense University's computer systems and as a result the University had to shut down its e-mail system.[47]

In November 2006, the Naval War College engaged in planning for naval warfare, cybersecurity and cyberwarfare had to go offline for two weeks because of a cyber-attack.[48]

In August 2006, a group of civilians in china engaged in writing malicious code, which could be set to cyber strike U.S. Defense Department, succeeded in downloading 10 to 20 terabytes of data from the NIPRNet (DoD's Non-Classified IP Router Network).[49]

United States Department of Education

[42] David Perera, *"24,000 Files Stolen from DoD Contractor in Single March Allack,"* Fierce Homeland Security, (July 17, 2011), http://www.fiercehomelandsecurity.com/story/24000-files-stolen-dod-contractor-single-march-attack/2011-07-17 (last visited Nov. 26, 2012).

[43] Celina Westervelt, *"Soldiers' Personal Information Stolen,"* KRQE News, (Jan. 13, 2011), http://www.krqe.com/dpp/news/local/southeast/soldiers'-personal-information-stolen- (last visited Nov. 14, 2012).

[44] Martin Evans, *"Army Warns Reservists of Identity Theft Threat,"* Newsday, (April 22, 2010), http://www.newsday.com/news/new-york/army-warns-reservists-of-identity-theft-threat-1.1876244 (last visited Nov. 28, 2012).

[45] Siobhan Gorman, Yochi J Dreazen, and August Cole, *"Insurgents Hack U.S. Drones,"* The Wall Street Journal, (Dec. 17, 2009), http://online.wsj.com/article/ SB126102247889095011.html (last visited Nov. 27, 2012).

[46] *"Significant Cyber Incidents Since 2006, "Center for Strategic and International Studies,"* (May 4, 2012), http://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf.

[47] Id.

[48] Josh Rogin, *"China Is Suspected of Hacking into Navy Site,"* Federal Computer Week, (Dec. 4, 2012), http://fcw.com/articles/2006/12/04/china-is-suspected-of-hacking-into-navy-site.aspx?sc_lang=en (last visited Nov. 25, 2012).

[49] Dawn S. Onley and Patience Wait, *"Red Strom Rising,"* Government Computer News, (Aug. 7, 2006), http://gcn.com/articles/2006/08/17/red-storm-rising.aspx (last visited Nov 25, 2012).

In August 2006, an unknown intruder stole grant reviewers' personal information from their data computers.[50]

United States Department of Energy

In October 2011, some unknown intruders successfully attacked NNSA, which was confirmed by the Energy Department through disclosure.[51]

In July 2011, two U.S. government-funded research laboratories, namely, Pacific Northwest National Laboratory in Richland Washington; Thomas Jefferson National Laboratory in Newport News, Virginia along with a defense contractor, namely, Batelle Corp that managed PNNL, were brought under a cyberattack that forced them to go offline and to shut down the internet access.[52]

In April 2011, a federal facility, namely, Oak Ridge National Laboratory (ORNL), home to powerful supercomputers, which is located in Tennessee and is funded by U.S. Department of Energy that conducted classified and unclassified energy and national security work for the federal government, was hacked. In the event, a few megabytes of data was stolen that forced this federal facility to disconnect Internet access to prevent them from exposing to further vulnerabilities to this sensitive government facility.[53]

In October 2007, Oak Redge National Labs' database was hacked through an email that affected more than thousand officers of the federal government facility.[54]

United States Department of Homeland Security

In February 2012, the Department of Homeland Security (DHS) was crashed down by the online collective known as Anonymous causing the Department's website, DHS.gov, to go offline.[55]

In May 2009, Harry McDavid, the chief information officer for Department of Homeland Security's Office of Operations Coordination and Planning, confirmed that the Homeland Security Information Network (HSIN), the Homeland Security Department's platform for sharing sensitive but unclassified data with state and local authorities, was hacked by some unknown intruders. In the event, files that contained administrative data like email address and telephone numbers of state and federal employees were found stolen.[56]

---

[50] Identity Theft Resource Center, *"2006 Breach List,"* (April 1, 2009), http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20061231.pdf

[51] *"Energy Department Discloses Cyber Attack,"* Reuters, (Oct. 24, 2011), http://www.foxbusiness.com/search-results/search?q=energy+department+discloses+cyber+attack (last visited Nov. 19, 2012).

[52] *"Government Facilities Targets of Cyber Attacks,"* Reuters, (July 6, 2011), http://ca.reuters.com/article/technologyNews/idCATRE7656M020110706 (last visited Nov. 19, 2012).

[53] Kim Zetter, "Top Federal Lab Hacked in Spear-Phishing Attack," Wired, (April 20, 2011), http://www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack/ (last visited Nov. 19, 2012).

[54] *"Significant Cyber Incidents Since 2006, "Center for Strategic and International Studies,"* (May 4, 2012), http://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf.

[55] *"Department of Homeland Security Website Hacked by Anonymous,"* Russia Today, (March 7, 2012), http://rt.com/usa/news/homeland-security-website-anonymous-473/ (last visited Nov. 19, 2012).

[56] Ben Bain, *"Information Sharing Platform Hacked,"* Federal Computer Week, (May 13, 2009), http://fcw.com/articles/2009/05/13/web-dhs-hsin-intrusion-hack.aspx?sc_lang=en (last visited Nov. 19, 2012).

In September 2007, Unisys Corp, a company hired to build, secure and manage information technology by installing network-intrusion detection devices on the unclassified computer system for the Transportation Security Administration and Department of Homeland Security headquarters, failed to detect a Chinese-language Website oriented cyber break-ins that affected dozens of computers stealing unknown amount of sensitive information. Unisys Corp in an attempt to cover-up for its deficiencies concealed the incident stating that the DHS had stopped paying Unisys for monitoring their security services.[57]

In June 2007, hackers in an attempt to steal passwords and other sensitive data launched rootkit, stealthy computer software, on two internal servers of Department of Homeland Security.[58]

CONCLUSION

The present situation of cyber security, demands strict responses by means of policies and laws concerning technology that govern cybersecurity. In framing new policies and laws significance must be given to protect citizens from the state of being enslaved by the threats that wait in the cyber world. Defending citizens liberty as well as protecting them from the disorder that originates from an act of cyber plundering must be addressed to reach the global expectation of cyber tranquility. One of the greatest challenges of cybersecurity that lie in front of us is to keep cyber data secure and protected while preserving the modern communication system that connects a person globally. In the present circumstances Congress is demanded to frame and adopt a 'Gate Keeping Regime' to secure the cyberspace in ways that could confront all the risks and threats by malignant hackers. One of the biggest challenges to remedy the present cybersecurity situation is to eliminate the loophole created by the ever-changing hi-tech Internet technology by inventing new, efficient, and reliable techniques that could help government, corporations, even an individual user, to protect and safeguard confidential information to flow freely in the present interconnected networks; meanwhile, abolishing the possibility of causing harm from criminal gangs or hackers existing in the world.

The problems related to the present cybersecurity involve all aspects of law in some ways, shape, or form. However, our efforts through cyber legislations are slow to respond to the threats involved as laws and policies continue to chase the challenges created by the modern technology and its development.

[57] Ellen Nakashima and Brian Kerbs, *"Contractor Blamed in DHS Data Breaches,"* The Washington Post, (Sep. 24, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471_pf.html (last visited Nov. 19, 2012).

[58] Robert Westervelt, *"DHS Suffered More than 800 Cyber Attacks in Two Years,"* Computer Weekly, (June 25, 2007), http://www.computerweekly.com/news/2240081110/DHS-suffered-more-than-800-cyber-attacks-in-two-years (last visited Nov. 19, 2012).